

944-004.047

U.S. Patent Application

Of

Timo Tervo

and

Marko Leukkunen

For

SMART TERMINAL REMOTE LOCK AND FORMAT

Exp. Mail No. EV 435647343 US

SMART TERMINAL REMOTE LOCK AND FORMAT

Field of the Invention

5 The present invention relates to wireless communication, and more particularly to preventing unauthorized use of a mobile terminal.

Background of the Invention

10 There are many smart phones and equivalent terminals on the market that are capable of handling a great deal of data. In many cases, this data is critical for the user and/or for the company that the user is working for. The size of these data streams will inevitably increase, and many new applications will be introduced for these terminals. Some of those new applications will handle data that includes secret material in formats such as Word, PowerPoint, and Excel.

15 Smart phones will be handling documents that are currently handled only by desktop and laptop devices. Currently, laptops are very well-protected against loss and theft, but for mobile terminals such as smart phones there is not yet any global solution that protects information stored in the mobile terminal in case the terminal is lost or stolen, while also guarding against unauthorized usage.

20 Methods are known for a network to lock a mobile terminal, using an international mobile station equipment identity (IMEI) or subscriber identity module (SIM). An example of present technology is *Helle* (U.S. Patent No. 6,662,023) which guards against unauthorized usage and employs a short messaging system, but is incapable of addressing protection of data within the terminal. Most known methods use an 25 operator-provided service, but that does not help to prevent unauthorized data access in the terminal.

Having a mobile terminal stolen or misplaced is in many ways similar to losing an automated teller machine (ATM) card, for example. Even though the ATM card is protected by a user password, it is still conceivable that a criminal who obtains the 30 card might find a way to use it, perhaps after having spied on the user to obtain the password. Therefore, it is wise to request that the bank cancel the user password. Likewise, a password alone is not enough to protect a mobile terminal, because a thief

might find a way to bypass, steal, or decipher the password. In some ways, a mobile terminal may be even more vulnerable than an ATM card, if the mobile terminal has valuable documents stored inside of it, whereas an ATM card is almost useless unless it is taken to an ATM machine in order to access a bank account. In this sense, losing the mobile terminal would be similar to losing a memory stick, CD-ROM, or multimedia card (MMC), in which considerable data may be stored.

Summary of the Invention

The present invention allows a user to easily, securely and quickly format his user data-area, and lock his terminal remotely, via a push message or via Synchronization Markup Language (SyncML) Device Management, in order to prevent unauthorized usage of the terminal. This invention thereby overcomes the problem encountered when the user has lost or forgotten the terminal, or when the terminal is stolen. In such a case, the terminal will be locked and/or the user data-area will be reformatted immediately, in order to prevent unauthorized usage and data leakage from this personal trusted device (PTD).

The present invention provides a method to remotely lock a terminal and format a user data-area by using a Push message or SyncML Device Management. This invention can be user-initiated, or be provided as a service by an operator, or by any corporate entity.

There are two preferred embodiments for implementing the present invention. The first embodiment is light and proprietary (LP). The LP method can be accomplished by sending remote commands to a terminal via an unconfirmed push message. This embodiment fits within the context of the push model standardized by the Wireless Application Protocol (WAP) forum and Open Mobile Alliance (OMA). The command format for this push message is, for example, as follows: user secret pin, command [format, lock]. This format can be encrypted with a symmetric algorithm that is built from a combination of the user personal identification number (PIN) and IMEI, or equivalents. This user PIN is something that the user feeds into the mobile terminal when he enables remote control functions from his terminal.

The other preferred embodiment for implementing the present invention is heavy and open (HO). This embodiment has the same functionality as the LP embodiment, but involves exploiting SyncML functions which require a device management (DM) feature in the terminal. This LP option consumes more memory compared to the push 5 method (LP), due to the size of SyncML DM. However, if a terminal program already has SyncML DM, then this HO option may be preferable to the LP option.

In any case, no matter which embodiment is used (e.g. LP or HO), the present invention entails terminal lock and user data-area handling that can be accomplished for example in a Symbian OS environment by exploiting current Symbian servers such 10 as FS32 (FileSystem). LP requires a light server implementation, and a connection to PushProxy or directly to a short message service center (SMSC). For HO, a terminal management server can be exploited.

Brief Description of the Drawings

15 FIG. 1 is a flow chart illustrating an embodiment of the present invention.

FIG. 2 is a block diagram of a mobile terminal according to the present invention.

FIG. 3 shows a high-level architecture of a light and proprietary (LP) embodiment of the present invention.

20

Detailed Description of the Invention

The light and proprietary (LP) embodiment of the present invention exploits smart messages that may be implemented as bearer-independent objects (BIO), or exploits unconfirmed wireless access protocol (WAP) push messaging. According to the 25 alternative heavy and open (HO) embodiment, implementation is accomplished according to SyncML Device Management.

SyncML DM is very memory-intensive, and many terminals will not be able to support this feature. If a mobile terminal already supports SyncML DM then this may be the most efficient of the two alternative preferred embodiments.

30 Referring now to FIG. 1, this flow chart illustrates a method according to an embodiment of the present invention. The user input 102 a mobile terminal identifier

(which may be as simple as a telephone number), plus a personal identification code that is different from a PIN used to operate the mobile terminal, and the user enters these inputs at a location separate from the mobile terminal, which has presumably been lost, misplaced, stolen, or the like. An attendant then receives 104 these user inputs entered in step 102. The attendant may be automated or human or both, and typically would be linked to the user by a telephone connection. The attendant will determine 106 whether the mobile terminal employs synchronization markup language device management. If so, then the attendant will send 108 a guard message using synchronization markup language DM, and will do so repeatedly until the guard message is acknowledged (this is the HO embodiment). However, if the mobile terminal does not employ synchronization markup language DM then the attendant will send 110 the guard message, repeatedly if necessary, using either WAP push messaging or smart message BIO (this is the LP embodiment). The mobile terminal will then authenticate 112 the guard message, which of course could entail verifying the non-operational PIN entered in step 102. If the guard message is authenticated, then the mobile terminal will lock communication and secure data 114. This will not necessarily completely prevent communication from the mobile terminal, but it will at least greatly restrict it, while also making stored data less accessible. Especially sensitive data (or all data) may be deleted, although the user may request that the sensitive data first be uploaded with encryption to the attendant (for safekeeping or transfer to the user), prior to its deletion from the mobile terminal.

A thief might try to remove a battery, or otherwise deprive the mobile terminal of power, in order to ensure that the mobile terminal cannot respond to any guard message, and cannot reveal its location. Therefore, a user may purchase a mobile terminal that is equipped with a small emergency power unit that cannot be easily removed; that small emergency power unit can provide sufficient power for the mobile terminal to respond to the guard message by at least locking communication and securing data, if not by uploading data that is subsequently secured (e.g. deleted).

Regarding message construction, in the LP embodiment, the message content required for terminal format or lock includes push message identifiers: generic push port and meta data (e.g. SecFL). The message content also includes a function:

<format> and/or <lock>. And, the message content includes the international mobile station equipment identity: <imei code>. Additionally, the message content includes the user personal PIN: <4-digits, not same as SIM PIN>. The message format could be, for example, extensible markup language (XML) or wireless binary extensible markup language (WBXML) depending upon the selected solution configuration.

Referring now to FIG. 2, this is a block diagram of a mobile terminal 200 according to an embodiment of the present invention. The transceiver 202 receives a guard message 204 which it passes along to an authentication unit 206. Upon authenticating the guard signal 204, the authentication unit provides an authentication signal 208 to a data securing mechanism 210 as well as to a communication locking mechanism 212. In response to the authentication signal 208, the data securing mechanism 210 secures at least some of the data in a data storage unit 216, for example by deleting that data after encrypting and uploading the data via the transceiver 202. The communication locking mechanism 212 will respond to the authentication signal 208 by sending a disabling signal 214 to the transceiver, so as to completely or partially disable the transceiver (e.g. by barring the transceiver from communicating with any phone number except an emergency number).

Turning now to FIG. 3, this is a high-level architecture of the light and proprietary (LP) embodiment of the present invention. Regarding requirements for the client and server software in the LP embodiment, the client software 310 allows the user to enable a remote format and lock service from the user interface of his terminal, including entry of the user personal PIN. The terminal software is subsequently executed when a new message is received with appropriate meta information (e.g. SecFL to push port). No user interface should be displayed when the new message is received, because an unauthorized person may be observing the user interface. When the new message is received, then the software verifies the IMEI and user personal PIN. If those are correct, then the terminal software executes functions requested by the content of the new message.

Regarding the server software 302 in the LP embodiment of the present invention, the server has a database that includes IMEI information of users' terminals. The

server software has an application programming interface (API) with a short message service center (i.e. an SMSC 306 such as a CIMD-type of SMSC). An attendant, such as an information technology (IT) staff person in the user's company or a telephone operator of a wireless service provider, is able to construct the message that will be

5 sent to the lost or stolen mobile terminal, using the IMEI and PIN that are told by the user to the attendant. Then the message will be sent to a number that is in the database (DB) with the IMEI, via the GSM network 308. This functionality could be easily built inside a manufacturer management system, integrated with other IT management systems, or implemented separately.

10 Regarding the heavy and open (HO) embodiment of the present invention, the same functionality as the LP embodiment can be achieved by exploiting Synchronization Markup Language (SyncML) device management (DM).

15 It is to be understood that all of the present figures, and the accompanying narrative discussions of best mode embodiments, do not purport to be completely rigorous treatments of the method, terminal, and system under consideration. A person skilled in the art will understand that the steps and signals of the present application represent general cause-and-effect relationships that do not exclude intermediate interactions of various types, and will further understand that the various steps and structures described in this application can be implemented by a variety of

20 different sequences and configurations, using various different combinations of hardware and software which need not be further detailed herein.